UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/517,539	03/02/2000	Simon Robert Walmsley	AUTH01US	4602

7590	10/08/2003

Kia Silverbrook
Silverbrook Research Pty Ltd
393 Darling Street
Balmain,   2041
AUSTRALIA

EXAMINER
NGUYEN, NGA B

ART UNIT	PAPER NUMBER
3628	

DATE MAILED: 10/08/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

Office Action Summary	Applicati n N . 09/517,539	Applicant(s) WALMSLEY ET AL.	
	Examin r Nga B. Nguyen	Art Unit 3628	

-- The MAILING DATE f this c mmunication appears on the cover sheet with the correspondence address --

P riod for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>02 March 2000</u> .

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disp sition of Claims

4)☒ Claim(s) <u>1-12</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-12</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

    If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Pri rity under 35 U.S.C. §§ 119 and 120

13)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☒ All   b)☐ Some *   c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☒ Certified copies of the priority documents have been received in Application No. <u>09/113,223</u> .

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

    a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) <u>2</u> .

4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: .

DETAILED ACTION

1.   This Office Action is the answer to the communication filed on March 2, 2000,

which paper has been placed of record in the file.

2.   Claims 1-12 are pending in this application.

Claim Objections

3.   Claims 6-12 are objected to under 37 CFR 1.75(c), as being of improper

dependent form for failing to further limit the subject matter of a previous claim.

Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s)

in proper dependent form, or rewrite the claim(s) in independent form. A proper

dependent claim shall not conceivably be infringed by anything that would not also

infringe the base claim. See MPEP 608.01(n), Section III. The system claims 6-12

infringe the protocol steps of claims 1-5 because they recite the means which are used

to perform the method of claims 1-5 (a trusted authentication chip, an untrusted

authentication chip, a random number generator, a comparison means). As a result,

claims 6-12 are improper dependent claims.

Double Patenting

4.   The nonstatutory double patenting rejection is based on a judicially created

doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the

unjustified or improper timewise extension of the "right to exclude" granted by a patent

and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11

F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225

USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA

1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, *In re Thorington*,

418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be

used to overcome an actual or provisional rejection based on a nonstatutory double

patenting ground provided the conflicting application or patent is shown to be commonly

owned with this application. See 37 CFR 1.130(b). Effective January 1, 1994, a

registered attorney or agent of record may sign a terminal disclaimer. A terminal

disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

5.   Claim 1 is provisionally rejected under the judicially created doctrine of

obviousness-type double patenting as being unpatentable over claim 1 of copending

Application No. 09/517,384. Although the conflicting claims are not identical, they are

not patentably distinct from each other because claim 1 of copending Application No.

09/517,384 discloses the validation protocol for determining whether an untrusted

authentication chip is valid using an asymmetric encryption function (a one-way

function).

This is a provisional obviousness-type double patenting rejection because the

conflicting claims have not in fact been patented.

Claim Rejections - 35 USC § 102

6.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public
> use or on sale in this country, more than one year prior to the date of application for patent in the United
> States.

7.   Claims 1-4, 6, 7, 11, and 12 are rejected under 35 U.S.C. 102(b) as being

anticipated by Abraham et al (hereinafter Abraham), U.S. Patent No. 4,799,061.

Regarding to claim 1, Abraham discloses a validation protocol for determining

whether an untrusted authentication chip (figure 1, the card 10 having a processor

(chip) 14) is valid, or not, including the steps of:

generating a random number in a trusted authentication chip (figure 1, the terminal

20 having a processor (chip) 24, column 3, lines 9-19, the random number is generated

and encrypted at the terminal and transmitted to the card);

applying a keyed one way function to the random number using a key to produce

an outcome, in both the trusted authentication chip and an untrusted authentication chip

(column 3, lines 9-35, applying DES encryption algorithm (one way function) to encrypt

the random number using the key K1 to produce the value X at the terminal, applying

DES encryption algorithm to decrypt the random number using the key K2 to produce

the value Y at the card);

comparing the outcomes produced in both the trusted and untrusted chips, and in

the event of a match considering the untrusted chip to be valid (column 3, lines 35-44);

otherwise considering the untrusted chip to be invalid (column 3, lines 44-46).

Regarding to claim 2, Abraham discloses the key is kept secret (column 3, lines 4-8).

Regarding to claim 3, Abraham discloses the domain of the random numbers generated is non-deterministic (column 3, lines 9-13, the random numbers generated is non-deterministic because each challenge requires the user of a new random number).

Regarding to claim 4, Abraham discloses the keyed on-way function is a symmetric cryptograph, a random number sequence, or a message authentication code (column 3, lines 15-18, DES encryption algorithm is symmetric cryptograph).

Regarding to claim 6, Abraham discloses a validation system includes:

a trusted authentication chip and an untrusted authentication chip (figure 1, the terminal 20 having a processor (chip) 24 and the card 10 having a processor (chip) 14);

the trusted authentication chip includes a random number generator a keyed one-way function and a key for the function (column 3, lines 9-19, the terminal 20 generates the random number and encrypts it using the key K1, column 6, lines 24-27, means for generating random number);

the untrusted authentication chip includes the keyed one way function and the key (column 3, lines 18-23, the card 10 decrypts the value X using DES algorithm using the secret key K2);

a comparison means compares the outcomes produced in both the trusted and untrusted chips, and in the even of a match the untrusted chip is considered to be valid (column 6, lines 28-30, means for comparing).

Claims 7, 11, 12 have similar limitations found in claims 2, 4, 5, discussed above,

therefore, are rejected by the same rationale.

Claim Rejections - 35 USC § 103

8.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

9.   Claims 5 and 8-10 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Abraham et al (hereinafter Abraham), U.S. Patent No. 4,799,061, in view of

Thomlinson et al (herein after Thomlinson), U.S. Patent No. 5,778,069.

Regarding to claim 5, Abraham discloses the one-way function is a symmetric

cryptographic function (column 3, lines 15-18, DES encryption algorithm is symmetric

cryptograph and one way function), but Abraham does not teach the key has a

minimum size of 128 bits. However, Thomlinson discloses the key has a minimum size

of 128 bits (column 5, lines 59-65). Therefore, it would have been obvious to modify

Abraham's to include the feature above for the security purpose because producing the

encryption and decryption keys with larger bits makes the unauthorized person cannot

easily to guess the keys.

Regarding to claims 8, 9, Abraham does not disclose the trusted authentication

chip contains a random function to produce random numbers from a seed, and the

function advances after every random number is produced so that the next random

number will be produced from a new seed, and for a group of authentication chips, each

chip has a different initial seed, so that the first call to each chip requesting a random

number will produce different results for each chip in the group. However, Thomlinson

discloses the trusted authentication chip contains a random function to produce random

numbers from a seed, and the function advances after every random number is

produced so that the next random number will be produced from a new seed (column 6,

lines 36-60). Moreover, it is well known to use a different initial seed for each chip in the

group of chip. Therefore, it would have been obvious to modify Abraham's to include the

features above for the purpose of providing high security level because each random

number is generated from a new seed and each chip has a different initial seed, thus

the unauthorized person cannot easily to predict the random number.

Regarding to claim 10, Abraham discloses the domain of the random numbers

generated is non-deterministic (column 3, lines 9-13, the random numbers generated is

non-deterministic because each challenge requires the user of a new random number).

Conclusion

10.   Claims 1-12 are rejected.

11.   The prior arts made of record and not relied upon is considered pertinent to

applicant's disclosure:

Bjerrum et al (US 5,311,595) discloses method of transferring data between

computer systems using electronic cards.

Ishii (US 5,768,389) discloses method and system for generation and management of secret key of public key cryptosystem.

Shin et al (US 5,987,134) discloses a device for authenticating user's access rights to resources.

12.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to examiner Nga B. Nguyen whose telephone number is (703) 306-2901. The examiner can normally be reached on Monday-Thursday from 9:00AM-6:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Hyung S. Sough can be reached on (703) 308-0505.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group receptionist whose telephone number is (703) 306-1113.

13.   Any response to this action should be mailed to:

> Commissioner of Patents and Trademarks
>
> C/o Technology Center 3600
>
> Washington, DC 20231

Or faxed to:

> (703) 872-9326 (for formal communication intended for entry),

or

> (703) 308-3691 (for informal or draft communication, please label
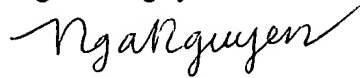
"PROPOSED" or "DRAFT").

Hand-delivered responses should be brought to Crystal Park 5, 2451 Crystal

Drive, Arlington, VA, Seventh Floor (Receptionist).

Nga B. Nguyen

September 29, 2003